

**WHAT IS CLAIMED IS:**

- 1           1.     A method of validating a user for a transaction to be  
2     effectuated by using a transaction card, comprising the steps of :  
3                 configuring a biometric profile for said user, said biometric  
4     profile including a plurality of biometric samples relating to said user;  
5                 associating said biometric profile with an indicium assigned  
6     to said transaction card;  
7                 biometrically interrogating said user when said transaction  
8     is attempted by said user;  
9                 monitoring a biometric response generated with respect to  
10    said user in response to said step of biometrical interrogation;  
11                determining if said biometric response matches a biometric  
12    sample in said biometric profile; and  
13                if so, approving said user for said transaction.

1           2.     The method of validating a user for a transaction as set forth  
2     in claim 1, wherein at least a portion of said plurality of biometric  
3     samples comprises voice samples generated by said user responsive to a  
4     plurality of questions directed to said user in said configuring step, and  
5     further wherein said step of biometrical interrogation involves querying  
6     said user for a voice response to a randomly selected question of said  
7     plurality of questions.

1           3.     The method of validating a user for a transaction as set forth  
2     in claim 1, further comprising the steps of:

3                 prompting said user to input said indicium assigned to said  
4     transaction card after determining that said biometric response matches  
5     a biometric sample of said biometric profile;

6                 determining if said indicium is a valid personal  
7     identification number operating as a password associated with said  
8     transaction card; and

9                 denying access to said user for said transaction if said  
10     indiciu is not a valid personal identification number associated with  
11     said transaction card.

1           4.     The method of validating a user for a transaction as set forth  
2     in claim 1, further comprising the steps of:

3                 prompting said user to input said indicium assigned to said  
4     transaction card if said biometric response does not match a biometric  
5     sample of said biometric profile;

6                 confirming that said indicium is a valid personal  
7     identification number associated with said transaction card; and

8                 approving said user for said transaction upon said  
9     confirmation.

1           5.     The method of validating a user for a transaction as set forth  
2     in claim 1, wherein the step of configuring a biometric profile for said  
3     user is effectuated manually.

1           6.     The method of validating a user for a transaction as set forth  
2     in claim 1, wherein the step of configuring a biometric profile for said  
3     user is effectuated automatically.

1           7.     The method of validating a user for a transaction as set forth  
2     in claim 1, further comprising the step of updating said biometric profile  
3     for said user.

1           8.     A method of validating a user for a call to be effectuated  
2 over a Public Switched Telephone Network (PSTN) using a calling card,  
3 comprising the steps of:

4                 configuring a personalized profile for said user, said  
5 personalized profile including a plurality of voice samples elicited from  
6 said user in response to a plurality of personalized questions directed to  
7 said user;

8                 associating said personalized profile with an indicium  
9 assigned to said calling card;

10                determining if a voice verification is needed with respect to  
11 said user when said call is attempted by said user;

12                if so, querying said user for a voice response to a question  
13 that is randomly selected from said plurality of personalized questions;

14                verifying if said voice response matches a corresponding  
15 voice sample in said voice profile; and

16                if so, approving said user for said call involving said calling  
17 card.

1           9.     The method of validating a user for a call as set forth in  
2     claim 8, further comprising the steps of:

3                 populating at least a portion of said personalized profile  
4     with a plurality of Dual Tone Multi Frequency (DTMF) sample  
5     responses elicited from said user in said configuration step;

6                 prompting said user to input a DTMF response in response  
7     to said question that is randomly selected from said plurality of  
8     personalized questions;

9                 verifying if said DTMF response matches a corresponding  
10    sample response in said personalized profile; and

11                denying access to said user for said call if said DTMF  
12    response does not match said corresponding sample response in said  
13    personalized profile.

1           10. The method of validating a user for a call as set forth in  
2 claim 8, further comprising the steps of:

3                 prompting said user to input said indicium assigned to said  
4 calling card after verifying that said voice response matches a  
5 corresponding voice sample in said voice profile;

6                 determining if said indicium is a valid personal  
7 identification number associated with said calling card; and

8                 denying access to said user for said call if said indicium is  
9 not a valid personal identification number associated with said calling  
10 card.

1           11. The method of validating a user for a call as set forth in  
2 claim 8, further comprising the steps of:

3                 prompting said user to input said indicium assigned to said  
4 calling card after verifying that said voice response does not match a  
5 corresponding voice sample in said voice profile;

6                 confirming that said indicium is a valid personal  
7 identification number associated with said calling card; and

8                 approving said user for said call upon said confirmation.

1           12. A fraud prevention method for use in a transaction-card-  
2 based system having a conventional authentication process, said  
3 comprising the steps of:

4                 determining, by utilizing said conventional authentication  
5 process, if a fraudulent transaction is being attempted in said transaction-  
6 card-based system by a user using a transaction card;

7                 if so, biometrically interrogating said user to obtain a  
8 biometric sample from said user; and

9                 upon obtaining said biometric sample, denying access to  
10 said user for said transaction in said transaction-card-based system if said  
11 biometric sample does not match an entry stored in a biometric profile  
12 database inherently associated with said transaction card's owner.

1           13. The fraud prevention method for use in a transaction-card-  
2 based system as set forth in claim 12, wherein said fraudulent transaction  
3 is selected from the group consisting of: placing a calling card call,  
4 accessing personal information data, accessing a bank account, accessing  
5 an Internet account, accessing a credit report, accessing employment  
6 records, and accessing medical records.

1           14. The fraud prevention method for use in a transaction-card-  
2 based system as set forth in claim 12, wherein said entry inherently  
3 associated with said transaction card's owner comprises a voiceprint  
4 associated with said owner.

1           15. The fraud prevention method for use in a transaction-card-  
2 based system as set forth in claim 12, wherein said entry inherently  
3 associated with said transaction card's owner comprises at least one of  
4 a fingerprint, retinal scan, palm print, and implanted ID chip associated  
5 with said owner.



1           16. An access control system for use with a transaction-card-  
2 based scheme, said system comprising:

3                 a network operable with a terminal, said terminal for  
4 interacting with a user in association with a transaction card;

5                 a controller disposed in the network to query said user when  
6 said user attempts a transaction using said transaction card;

7                 a server disposed in the network, said server responding to  
8 messages from said controller with respect to querying said user; and

9                 a profile database coupled to said server, said profile  
10 database having a plurality of biometric samples inherently coupled to  
11 said user, wherein said biometric samples are associated with an  
12 indicium assigned to said transaction card such that when said user  
13 attempts said transaction, said controller queries said user for a response  
14 thereto and if said response does not match a corresponding entry in said  
15 profile database, access is denied to said user for said transaction.

1           17. The access control system for use with a transaction-card-  
2 based scheme as set forth in claim 16, wherein said entry inherently  
3 coupled to said user comprises at least one of a fingerprint, retinal scan,  
4 palm print, and implanted ID chip associated with said user.

1           22.    The access control system for use with a transaction-card-  
2           based scheme as set forth in claim 16, wherein said terminal comprises  
3           a wireless medium device.